TOLER SCHAFFER, LLP
8500 Bluffstone Cove, Suite A201
Austin, Texas 78759
Phone 512-327-5515
Fax 512-327-5575

RECEIVED
CENTRAL FAX CENTER
FEB 2 8 2007

FACSIMILE COVER SHEET

DATE: February 28, 2007

TO: Examiner HOANG, Daniel L. **FAX NO.:** 571-273-8300
USPTO GPAU 2136

FROM: Jeffrey G. Toler
Reg. No.: 38,342

RE U.S. App. No.: 10/634,117, filed August 4, 2003

Applicant(s): James M. Doherty, et al.

Atty Dkt No.: 1033-T00534

Title: HOST INTRUSION DETECTION AND ISOLATION

NO. OF PAGES (including Cover Sheet): 21

MESSAGE:

Attached please find:

☒ Transmittal Form (1 pg)
☒ Fee Transmittal [in duplicate] (2 pgs)
☒ Brief in Support of Appeal (17 pgs)

8500 Bluffstone Cove
Suite A201
AUSTIN, TEXAS 78759

Tel: (512) 327-5515
Fax: (512) 327-5575

RECEIVED
CENTRAL FAX CENTER
FEB 2 8 2007

PTO/SB/21 (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission: 21

Application Number	10/634,117
Filing Date	August 4, 2003
First Named Inventor	James M. Doherty, et al.
Art Unit	2136
Examiner Name	HOANG, Daniel L.
Attorney Docket Number	1033-T00534

ENCLOSURES *(Check all that apply)*

- [x] Fee Transmittal Form
  - [ ] Fee Attached
- [ ] Amendment/Reply
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [ ] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [ ] Reply to Missing Parts/ Incomplete Application
  - [ ] Reply to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) _____
  - [ ] Landscape Table on CD
- [ ] After Allowance Communication to TC
- [ ] Appeal Communication to Board of Appeals and Interferences
- [x] Appeal Communication to TC (Appeal Notice, Brief, Reply Brief)
- [ ] Proprietary Information
- [ ] Status Letter
- [ ] Other Enclosure(s) (please identify below):

Remarks

Customer No.: 60533

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	Toler Schaffer, LLP		
Signature			
Printed name	Jeffrey G. Toler		
Date	2-28-2007	Reg. No.	38,342

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature			
Typed or printed name	Jeaneaux Jordan	Date	2-28-07

RECEIVED
CENTRAL FAX CENTER
FEB 2 8 2007

PTO/SB/17 (02-07)
Approved for use through 02/28/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Effective on 12/08/2004.
Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).

FEE TRANSMITTAL
For FY 2007

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 500.00

Complete if Known	
Application Number	10/634,117
Filing Date	August 4, 2003
First Named Inventor	James M. Doherty, et al.
Examiner Name	HOANG, Daniel L.
Art Unit	2136
Attorney Docket No.	1033-T00534

METHOD OF PAYMENT (check all that apply)

☐ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please identify): _____

☑ Deposit Account Deposit Account Number: 50-2469 Deposit Account Name: Toler Schaffer, LLP

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☑ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, except for the filing fee

☐ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17 ☑ Credit any overpayments

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

Application Type	FILING FEES Fee ($)	FILING FEES Small Entity Fee ($)	SEARCH FEES Fee ($)	SEARCH FEES Small Entity Fee ($)	EXAMINATION FEES Fee ($)	EXAMINATION FEES Small Entity Fee ($)	Fees Paid ($)
Utility	300	150	500	250	200	100	
Design	200	100	100	50	130	65	
Plant	200	100	300	150	160	80	
Reissue	300	150	500	250	600	300	
Provisional	200	100	0	0	0	0	

2. EXCESS CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20 (including Reissues)	50	25
Each independent claim over 3 (including Reissues)	200	100
Multiple dependent claims	360	180

Total Claims _____ - 20 or HP = _____ Extra Claims _____ x Fee ($) _____ = Fee Paid ($) _____

HP = highest number of total claims paid for, if greater than 20.

Indep. Claims _____ - 3 or HP = _____ Extra Claims _____ x Fee ($) _____ = Fee Paid ($) _____

HP = highest number of independent claims paid for, if greater than 3.

Multiple Dependent Claims Fee ($) _____ Fee Paid ($) _____

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets _____ - 100 = _____ Extra Sheets _____ / 50 = _____ Number of each additional 50 or fraction thereof (round up to a whole number) x Fee ($) _____ = Fee Paid ($) _____

4. OTHER FEE(S)

	Fees Paid ($)
Non-English Specification, $130 fee (no small entity discount)	
Other (e.g., late filing surcharge): Brief in Support of Appeal	500.00

SUBMITTED BY

Signature		Registration No. (Attorney/Agent) 38,342	Telephone 512-327-5515
Name (Print/Type)	Jeffrey G. Toler		Date 2-28-2007

RECEIVED
CENTRAL FAX CENTER
FEB 2 8 2007

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	**James M. Doherty, et al.**		
Title:	**HOST INTRUSION DETECTION AND ISOLATION**		
App. No.:	**10/634,117**	Filed:	**August 4, 2003**
Examiner:	**HOANG, Daniel L.**	Group Art Unit:	**2136**
Customer No.:	**60533**	Confirmation No.:	**5753**
Atty. Dkt. No.:	**1033-T00534**		

BOARD OF PATENT APPEALS
AND INTERFERENCES
United States Patent
and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

BRIEF IN SUPPORT OF APPEAL

Jeffrey G. Toler, Reg. No. 38,342
Attorney for Appellant
TOLER SCHAFFER, LLP
8500 Bluffstone Cove, Suite A201
Austin, Texas 78759
(512) 327-5515 (phone)
(512) 327-5575 (fax)

03/01/2007 TL0111 00000038 502469 10634117
01 FC:1402 500.00 DA

I. REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))

The Real Party in Interest in the present Appeal is **SBC Knowledge Ventures, L.P.**, the assignee, of patent application no. **10/634,117**, as evidenced by the assignment set forth at Reel **014326**, Frame **0580**.

II. RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 41.37(c)(1)(ii))

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in this appeal, Appellant is not aware of any such appeals or interferences.

III. STATUS OF CLAIMS (37 C.F.R. § 41.37(c)(1)(iii))

A. Total Number of Claims in Application

There are 25 claims pending in the application (claims 1, 3-15, and 17-27).

B. Status of All the Claims

Claims 1, 14, and 15 are independent claims. According to pages 2-7 of the Final Office Action dated October 18, 2006, the Examiner states that claims 1, 3-15, and 17-27 stand rejected, and are hereby appealed. Claims 2 and 16 were canceled in the Amendment filed September 12, 2006.

C. Claims on Appeal

There are 25 claims on appeal (claims 1, 3-15 and 17-27).

IV. STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))

The claims hereby Appealed are based on the Amendment filed September 12, 2006. No amendment was offered or entered after the Final Office Action.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER (37 C.F.R. § 41.37(c)(1)(v))

The subject matter of claim 1 can be summarized as follows:

A method is disclosed that includes providing a host computer system having at least one network interface interfaced with a computer network, operating the host computer system in a multi-user mode, and detecting an intrusion event using a system daemon. The method further includes, in response to detecting the intrusion event, isolating the at least one network interface from the computer network and taking the host computer system down to a single user state so that access to the host computer system is limited to physical access at the host computer system.

Claim 1 finds support from at least FIGS. 1 and 2 and on page 2, paragraphs 1009 and 1010 and page 4, paragraph 1018 through page 5, paragraph 1022 of the specification.

The subject matter of claim 14 can be summarized as follows:

A method is disclosed that includes providing a host computer system having at least one network interface interfaced with a computer network, operating the host computer system in a multi-user mode, executing a system daemon on the host computer system, and reading, by the system daemon, a configuration file that indicates at least one file in a file system of the host computer system to be monitored for intrusion. The configuration file includes a first directive type that indicates a directory whose members are to be monitored for intrusion, a second directive type that indicates a file to be monitored for intrusion, and a third directive type that indicates another configuration file to be monitored for intrusion. The method further includes reading a valid MD5 signature for a monitored file from a database that is located on a second computer system isolated physically and programmatically from the host computer system and detecting an intrusion event using the system daemon by detecting that an MD5 signature of the monitored file differs from the valid MD5 signature. Additionally, the method includes, in

response to detecting the intrusion event, issuing an IFCONFIG down command to the at least one network interface to isolate the at least one network interface from the computer network, issuing an INIT1 command to an operating system of the host computer system to take the host computer system down to a single user state, and writing a log of the intrusion event to a log database that is not located on the second computer system.

Claim 14 finds support from at least FIGS. 1 and 2 and on page 2, paragraphs 1009 and 1010 and page 4, paragraph 1018 through page 5, paragraph 1022 of the specification.

The subject matter of claim 15 can be summarized as follows:

A system is disclosed that includes a host computer system having at least one network interface interfaced with a computer network. The host computer system operates in a multi-user mode and detects an intrusion event using a system daemon. In response to detecting the intrusion event, the host computer system isolates the at least one network interface from the computer network and takes the host computer system down to a single user state so that access to the host computer system is limited to physical access at the host computer system.

Claim 15 finds support from at least FIGS. 1 and 2 and on page 2, paragraphs 1009 and 1010 and page 4, paragraph 1018 through page 5, paragraph 1022 of the specification.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL (37 C.F.R. § 41.37(c)(1)(vi))

Claims 1, 3-27 are rejected under 35 U.S.C. 103(a) as being anticipated over U.S. Patent Publication No. 2004/0049693 ("Douglas") in view of U.S. Patent No. 6,081,894 ("Mann").

VII. ARGUMENT (37 C.F.R. § 41.37(c)(1)(vii))

Appellant respectfully appeals each of the rejections applied against all claims now pending on appeal.

CLAIMS 1 and 3-13 ARE ALLOWABLE OVER DOUGLAS AND MANN

Appellant respectfully traverses the rejection of claims 1 and 3-13 under 35 U.S.C.§103(a) over U.S. Patent Publication No. 2004/0049693 ("Douglas") in view of U.S. Patent No. 6,081,894 ("Mann"), at page 3 of the Final Office Action. The Final Office Action acknowledges (*Final Office Action*, pp. 3-4) that Douglas does not disclose or suggest, "in response to detecting an intrusion event, isolating at least one network interface from a computer network and taking a host system down to a single user state so that access to the host computer system is limited to physical access at the host computer system," as recited by independent claim 1.

The Final Office Action asserts that Mann discloses this feature, citing Mann at col. 3, lines 2-5. At the section referenced by the Final Office Action, Mann states:

> When a virus is detected, a data isolator 60, that is responsive to a control signal 42 from the data comparator 40, isolates the first data channel 22 from the second data channel 32. Thus, viruses are detected and prevented from being received by the data receiving entity 30.

Mann, col. 3, lines 2-5. Thus, the data isolator of Mann resides between the data receiving entity (e.g., personal computer or local area network) and the data sending entity (i.e. the internet). *See Mann*, col. 2, line 61 through col. 3, line 7. However, Mann discloses that the data sending entity is isolated from the data receiving entity without disrupting normal operation of either entity. *See Mann*, col. 2, lines 30-32 (emphasis added).

Appellant notes that claim 1 recites "operating the host computer in a multi-user mode" and "a host computer system to operate in a multi-user mode," respectively. Additionally, independent claim 1 recites "in response to detecting the intrusion event, isolating the at least one network interface from the computer network and taking the host computer system down to a single user state so that access to the host computer system is limited to physical access at the host computer system." The "single user state" is a different state from normal operation ("multi-user mode"). Thus, Mann does not disclose or suggest taking the host computer system down to a single user state, as recited by independent claim 1.

The Final Office Action states:

> When the first data channel is isolated from the second data channel, it is obvious that the two entities are isolated from each other. Because there are only two entities and they are isolated from each other, it is clear that both entities are in single user states.

The Final Office Action, p. 2.

The assumption that "it is clear that both entities are in single user states" is incorrect and not applicable, since neither the "data isolator" nor the "data receiving entity" of Mann are indicated to be in a multi-user state. Moreover, the data sending entity is indicated to be the Internet (*See Mann*, col. 2, lines 62-63), so it is unclear how the data sending entity could ever be reduced to a single user state.

Further, Mann discloses that the isolation is provided without disrupting normal operation. *See Mann*, col. 2, lines 30-32. In direct contrast, claim 1 recites "taking the host computer system down to a single user state." Altering the state of the device from a multi-user state to a single user state is a disruption of normal operation. Thus, Mann teaches away from claim 1.

Moreover, Mann discloses that the data receiving entity may be a personal computer or a local area network. *See Mann*, col. 2, lines 63-64. Mann provides no indication that the personal computer operates in a multi-user mode and provides no indication that the data isolator is adapted to take the receiving device down to a single user state. When the receiving device is a

local area network, it is unclear how the local area network may be reduced to a single user state without disruption of normal operation. Further, Mann does not disclose or suggest any direct action taken with respect to the data receiving entity. Instead, Mann discloses that the data isolator isolates the data receiving entity by isolating a first data channel (extending from the data sending entity to the data isolator) from a second data channel (extending from the data isolator to the data receiving device). *See Mann*, Figure 1, Abstract, and col. 2, line 61 through col. 3, line 5.

Thus, Mann does not disclose or suggest "taking the host computer system down to a single user state," as recited by claim 1. Therefore, Mann fails to overcome the deficiencies of Douglas, and the asserted combination of Douglas and Mann fails to disclose or suggest each and every element of independent claim 1, and of dependent claims 3-13, at least by virtue of their dependency from allowable claim 1. At least for the foregoing reasons, the rejection of claims 1, and 3-13 should be withdrawn.

Additionally, dependent claim 4 provides an additional basis for patentability over the cited references. For example, the asserted combination of Douglas and Mann fails to disclose or suggest that "taking the host computer system down to the single user state comprises issuing an INIT1 command to an operating system of the host computer system," as recited by claim 4. Instead, neither Douglas nor Mann disclose taking the host computer system down to the single user state. Moreover, to the extent that Mann discloses isolation, such isolation is achieved by activating a data isolator and without issuing commands to a host computer system. *See Mann*, Figure 1 and Abstract. Thus, Douglas and Mann do not disclose the particular combination of claim 4.

For at least the foregoing reasons, the rejection of claims 1 and 3-13 should be withdrawn.

CLAIMS 15 and 17-27 ARE ALLOWABLE OVER DOUGLAS AND MANN

Appellant respectfully traverses the rejection of claims 15 and 17-27 under 35 U.S.C.§103(a) over Douglas and Mann, at page 3 of the Final Office Action. The Final Office

Action acknowledges (*Final Office Action*, pp. 3-4) that Douglas does not disclose or suggest, "in response to detecting an intrusion event, isolating at least one network interface from a computer network and taking a host system down to a single user state so that access to the host computer system is limited to physical access at the host computer system," as recited by independent claim 15.

Claim 15 recites a system that includes "a host computer system having at least one network interface interfaced with a computer network," where the host computer system is to "operate in a multi-user mode," "detect an intrusion event using a system daemon," and "in response to detecting the intrusion event, isolate the at least one network interface from the computer network and take the host computer system down to a single user state so that access to the host computer system is limited to physical access at the host computer system."

As discussed above with respect to claim 1, the Final Office Action acknowledges that Douglas fails to disclose or suggest a system that, "in response to detecting the intrusion event, isolate the at least one network interface from the computer network and take the host computer system down to a single user state so that access to the host computer system is limited to physical access at the host computer system," as recited by claim 15. Mann fails to overcome the deficiencies of Douglas, because, not only does Mann disclose isolating the sending and receiving entities without disrupting normal operation (*See Mann*, col. 2, lines 30-32), but Mann fails to disclose or suggest a "single user state" for the sending or the receiving entities. Moreover, Mann fails to disclose or suggest that the data isolation apparatus can operate in a multi-user mode. Thus, the asserted combination of Douglas and Mann fails to disclose or suggest the particular combination of claim 15.

Thus, the asserted combination of Douglas and Mann does not disclose or suggest each and every element of claim 15, or of claims 17-27 at least by virtue of their dependency from allowable claim 15.

For at least the foregoing reasons, the rejection of claims 15 and 17-27 over Douglas and Mann should be withdrawn.

CLAIM 14 IS ALLOWABLE OVER DOUGLAS AND MANN

Appellant respectfully traverses the rejection of claim 14 under 35 U.S.C. §103(a) over Douglas in view of Mann at pages 3 and 6 of the Final Office Action. None of the cited references, alone or in combination, recite the particular combination of independent claim 14.

The Final Office Action states that claim 14 "is rejected by Douglas and Mann as applied to claims 1-8 and 10." *See Final Office Action*, p. 6. However, the Final Office Action fails to indicate the particular bases for the rejection, and the Appellant is left to guess as to how the Office is interpreting the references to apply to the actual claim language. Appellant notes that claim 14 recites:

> A method comprising:
> providing a host computer system having at least one network interface interfaced with a computer network;
> operating the host computer system in a multi-user mode;
> executing a system daemon on the host computer system;
> reading, by the system daemon, a configuration file that indicates at least one file in a file system of the host computer system to be monitored for intrusion, wherein the configuration file comprises a first directive type that indicates a directory whose members are to be monitored for intrusion, a second directive type that indicates a file to be monitored for intrusion, and a third directive type that indicates another configuration file to be monitored for intrusion;
> reading a valid MD5 signature for a monitored file from a database that is located on a second computer system isolated physically and programmatically from the host computer system;
> detecting an intrusion event using the system daemon by detecting that an MD5 signature of the monitored file differs from the valid MD5 signature; and
> in response to detecting the intrusion event:
> issuing an IFCONFIG down command to the at least one network interface to isolate the at least one network interface from the computer network;
> issuing an INIT1 command to an operating system of the host computer system to take the host computer system down to a single user state; and
> writing a log of the intrusion event to a log database that is not located on the second computer system.

The cited references, alone or in combination, do not disclose or suggest the particular combination of claim 14. For example, as described above, the asserted combination of Douglas and Mann fails to disclose or suggest a method that includes "operating the host computer system in a multi-user mode" and, "in response to detecting the intrusion event," "issuing an

INIT1 command to an operating system of the host computer system to take the host computer system down to a single user state," as recited in claim 14.

As previously discussed, Douglas fails to disclose or suggest, in response to detecting an intrusion event, taking the host computer down to a single user state. Also, as previously discussed, Mann provides no indication that any of the sending entity, the receiving entity, or the data isolator operates in a multi-user mode. Further, Mann provides no indication that the data isolator is adapted to take the receiving device down to a single user state. Moreover, Mann does not disclose or suggest issuing an INIT1 command to an operating system of the host computer system to take the host computer system down to a single user state, as recited by claim 14. Instead, Mann provides isolation by providing power to the data isolator to isolate the first data channel from the second data channel. *See Mann*, Abstract, and col. 2, line 61 through col. 3, line 5. Thus, the asserted combination of Douglas and Mann fails to disclose or suggest at least one element of independent claim 14. Therefore, the rejection of claim 14 should be withdrawn.

For at least the foregoing reasons, Appellant respectfully submits that the present application is in condition for allowance and reconsideration is respectfully requested.

VIII. CLAIMS APPENDIX (37 C.F.R. § 41.37(c)(1)(viii))

The text of each claim involved in the appeal is as follows:

1. (Original) A method comprising:

providing a host computer system having at least one network interface interfaced with a computer network;

operating the host computer system in a multi-user mode;

detecting an intrusion event using a system daemon; and

in response to detecting the intrusion event, isolating the at least one network interface from the computer network and taking the host computer system down to a single user state so that access to the host computer system is limited to physical access at the host computer system.

2. (Canceled).

3. (Original) The method of claim 1 wherein said isolating the at least one network interface from the computer network comprises issuing an IFCONFIG down command to the at least one network interface.

4. (Original) The method of claim 1 wherein said taking the host computer system down to the single user state comprises issuing an INIT1 command to an operating system of the host computer system.

5. (Original) The method of claim 1 further comprising:

reading, by the system daemon, a configuration file that indicates at least one file in a file system of the host computer system to be monitored for intrusion.

6. (Original) The method of claim 5 wherein the configuration file comprises a first directive type that indicates a directory whose members are to be monitored for intrusion, a second directive type that indicates a file to be monitored for intrusion, and a third directive type that indicates another configuration file to be monitored for intrusion.

7. (Original) The method of claim 1 further comprising:

computing a data verification signature for a monitored file in a file system of the host computer system; and

comparing the data verification signature to a valid data verification signature for the monitored file;

wherein said detecting the intrusion event comprises detecting that the data verification signature differs from the valid data verification signature.

8. (Original) The method of claim 7 wherein the valid data verification signature comprises a Message Digest 5 (MD5) signature.

9. (Original) The method of claim 7 further comprising:

reading the valid data verification signature for the monitored file from a database that is located on a second computer system isolated physically and programmatically from the host computer system.

10. (Original) The method of claim 9 further comprising:

writing a log of the intrusion event to a log database that is not located on the host computer system or second computer system.

11. (Original) The method of claim 1 wherein said detecting the intrusion event comprises detecting an incorrect permission associated with a file in a file system of the host computer system.

12. (Original) The method of claim 1 wherein said detecting the intrusion event comprises detecting an incorrect ownership associated with a file in a file system of the host computer system.

13. (Original) The method of claim 1 wherein said detecting the intrusion event comprises detecting that a file no longer exists in a file system of the host computer system.

14. (Previously Presented) A method comprising:

providing a host computer system having at least one network interface interfaced with a computer network;

operating the host computer system in a multi-user mode;

executing a system daemon on the host computer system;

reading, by the system daemon, a configuration file that indicates at least one file in a file system of the host computer system to be monitored for intrusion, wherein the configuration file comprises a first directive type that indicates a directory whose members are to be monitored for intrusion, a second directive type that indicates a file to be monitored for intrusion, and a third directive type that indicates another configuration file to be monitored for intrusion;

reading a valid MD5 signature for a monitored file from a database that is located on a second computer system isolated physically and programmatically from the host computer system;

detecting an intrusion event using the system daemon by detecting that an MD5 signature of the monitored file differs from the valid MD5 signature; and

in response to detecting the intrusion event:

issuing an IFCONFIG down command to the at least one network interface to isolate the at least one network interface from the computer network;

issuing an INIT1 command to an operating system of the host computer system to take the host computer system down to a single user state; and

writing a log of the intrusion event to a log database that is not located on the second computer system.

15. (Original) A system comprising:

a host computer system having at least one network interface interfaced with a computer network, the host computer system to:

operate in a multi-user mode;

detect an intrusion event using a system daemon; and

in response to detecting the intrusion event, isolate the at least one network interface from the computer network and take the host computer system down to a single user state so that access to the host computer system is limited to physical access at the host computer system.

16. (Canceled).

17. (Original) The system of claim 15 wherein the host computer system is to isolate the at least one network interface from the computer network by issuing an IFCONFIG down command to the at least one network interface.

18. (Original) The system of claim 15 wherein the host computer system is taken down to the single user state by issuing an INIT1 command to an operating system of the host computer system.

19. (Original) The system of claim 15 wherein the host computer system is further to read, by the system daemon, a configuration file that indicates at least one file in a file system of the host computer system to be monitored for intrusion.

20. (Original) The system of claim 19 wherein the configuration file comprises a first directive type that indicates a directory whose members are to be monitored for intrusion, a second directive type that indicates a file to be monitored for intrusion, and a third directive type that indicates another configuration file to be monitored for intrusion.

21. (Original) The system of claim 15 wherein the host computer system is further to:

compute a data verification signature for a monitored file in a file system of the host computer system; and

compare the data verification signature to a valid data verification signature for the monitored file;

wherein the intrusion event is detected by detecting that the data verification signature differs from the valid data verification signature.

22. (Original) The system of claim 21 wherein the valid data verification signature comprises a Message Digest 5 (MD5) signature.

23. (Original) The system of claim 21 further comprising:

a second computer system isolated physically and programmatically from the host computer system;

wherein the host computer system is to read the valid data verification signature for the monitored file from a database that is located on the second computer system.

24. (Original) The system of claim 23 further comprising:

a log database not located on the host computer system or the second computer system;

wherein the host computer system is further to write a log of the intrusion event to the log database.

25. (Original) The system of claim 15 wherein the intrusion event comprises an incorrect permission associated with a file in a file system of the host computer system.

26. (Original) The system of claim 15 wherein the intrusion event comprises an incorrect ownership associated with a file in a file system of the host computer system.

27. (Original) The system of claim 15 wherein the intrusion event comprises a file no longer existing in a file system of the host computer system.

IX. EVIDENCE APPENDIX (37 C.F.R. § 41.37(c)(1)(ix))

(N/A)

X. RELATED PROCEEDINGS APPENDIX (37 C.F.R. § 41.37(c)(1)(x))

(N/A)

XI. CONCLUSION

For at least the above reasons, all pending claims are allowable and a notice of allowance is courteously solicited. Please direct any questions or comments to the undersigned attorney at the address indicated. Appellant respectfully requests reconsideration and allowance of all claims and that this patent application be passed to issue.

Respectfully submitted,

2-28-2007
Date

Jeffrey G. Toler; Reg. No. 38,342
Attorney for Appellant
TOLER SCHAFFER, L.L.P.
8500 Bluffstone Cove, Suite A201
Austin, Texas 78759
(512) 327-5515 (phone)
(512) 327-5575 (fax)

JGT/RMR